UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/784,254	02/16/2001	Soichi Furuya	520.39632X00	6139

20457 7590 09/09/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	5

DATE MAILED: 09/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/784,254	**Applicant(s)** FURUYA ET AL.	
	Examiner Ellen C Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 February 2001_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-8,13-20,25-32 and 37_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-8,13-20,25-32 and 37_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _4_.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 16 February 2001, with acknowledgement of foreign application date of 09 March 2000.

2. Acknowledgement of Pre-Amendment filed 28 March 2001, claims 9-12, 21-24, and 33-36 are withdrawn.

3. Claims 1-8, 13-20, 25-32, and 37 are currently pending in this application. Claims 1, 13, 25, and 37 are independent claims.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-8, 13-20, 25-32, and 37are** rejected under 35 U.S.C. 103(a) as being unpatentable over Djakovic U.S. Patent No. 6,351,539 (hereinafter '539) in further view of Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter '095).

As to independent claim 1, "A symmetric-key encryption method comprising the steps of: dividing plaintext composed of redundancy data" is taught in '539 col. 2, lines 9-19 " This invention solves these and other problems by providing a combination block ciper with an effective key length greater than that of its components … a one-time pad in the form of a random data stream is combined with an encrypted form of the input stream before it is encrypted by the second block cipher"

"generating a random number sequence based on a secret key; generating a random number block corresponding to one of said plurality of plaintext blocks from said random number sequence" is shown in '539, col. 2, lines 19-26 "In one aspect, this invention is an encryption device which has a random number generator and three block cipher mechanisms ... An exclusive-or mechanism takes as input the first enciphered output from the first block cipher and output of the random number generator and produces a combined output";

"outputting a feedback value obtained as a result of operation on said one of the plurality of plaintext blocks and said random number block, said feedback value being fed back to another one of the plurality of plaintext blocks; and performing an encryption operation using said one of the plurality of plaintext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of plaintext blocks to produce a ciphertext block" is disclosed in '539 col. 2, lines 26-36 "The second block cipher mechanism takes as input the output of the exclusive-or mechanism and produces a second enciphered output based on the output of exclusive-or mechanism and on a second key";

the following is not taught in '539 however '095 teaches

"and a message to generate a plurality of plaintext blocks each having a predetermined length" in col. 5, lines 52-67 "A further object of the present invention is to provide a technique whereby the cipher uses a variable number of stages (and therefore rounds) of processing during encryption"

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '539 that shown a cipher mixer with a random number generator to include the capability to divide the message or data into a plurality of blocks. One of ordinary skill in the art would have been motivated to perform such a modification to increase the difficulty of decoding private information transmitted. As indicated by '095 (see col. 3, lines 65 et seq.) "In view of the above, a stronger, more flexible cipher is needed. One way to make a cipher stronger is to increase the number of rounds of ciphering performed: with each successive transformation, the resulting encryption becomes more difficult to break".

As to dependent claim 2, "wherein said encryption operation uses one or more said random number blocks whose total length is longer than a length of said ciphertext block" is taught in '539, col. 2, lines 50-52 "The effective key length is the sum of key lengths used in BC1 and BC2 (256 in the preferred scheme).".

As to dependent claim 3, "wherein said plaintext further includes secret data of a predetermined length" is shown in '539 col. 4, lines 1-3 "In the operation, a plaintext input stream P is input to block cipher BC1 18 which operates on it (in encrypting mode) using the 128-bit key K1 to produce a sequence" (i.e. "plaintext same as "input stream"/ "secret data of predetermine length" same as "128 bit key")

As to dependent claim 4, "wherein said encryption operation performs a binomial operation or a monomial operation using one of said plurality of plaintext blocks one or more times according to a predetermined procedure, combines a plurality of obtained

ciphertext blocks, and outputs the combined plurality of ciphertext blocks as ciphertext" is disclosed in '539 col. 4, lines 14-25 "The sequence SR of random numbers produced by the RNG 14 is also input to block ciper BC3 22 which uses the 256-bit key K3 (in encrypting mode) to produce and encciptered random sequence of 64-bit values (denoted SER=BC3(SR, K3))."

As to dependent claim 5, **"wherein said encryption operation includes multiplication and addition in a finite field"** is taught in '539 col. 4, lines 14-25 "The sequence SR of random numbers produced by the RNG 14 is also input to block ciper BC3 22 which uses the 256-bit key K3 (in encrypting mode) to produce and enciphered random sequence of 64-bit values (denoted SER=BC3(SR, K3))."

As to dependent claim 6, **"wherein said encryption operation includes a combination of a cyclic shift operation and arithmetic multiplication"** is shown in '539 col. 4, lines 45-55 "That is, the plaintext is produced by BC1 (S1, K1). The output of the decryptor mechanism 26 can be denoted: … where the input stream to the decryptor mechanism 26 is a combination of the two sequences SER and S3 , and where SER and S3 can be extracted from the input stream".

As to dependent claim 7, **"wherein said symmetric-key encryption method employs a pseudorandom-number generating means for generating said random number sequence based on said secret key"** is disclosed in '095 col. 6, lines 29-38 "To achieve the foregoing objects, and in accordance with the purpose of the invention a broadly described herein, the present invention provides a technique, system and method for implement a symmetric key block cipher supporting a variable number of stages, variable length input key, a variable length block, and a variable number of rounds, and the rounds have a plurality of subrounds comprising: a subprocess for generating a plurality of subkeys using the input key and a first pseudorandom function".

As to dependent claim 8, **"further comprising steps of: dividing said message into a plurality of message blocks; generating a number of random number sequences equal to the number of said plurality of message blocks using said pseudorandom-number generating means; and"** is taught in '095 col. 11, lines 1-25 "In the preferred embodiment, key setup is performed by filling the expanded key array with values generated using iterated pseudorandom functions that use a counter, I, and the input key K as parameters, as specified following pseudo-code:";

"performing parallel processing by assigning said plurality of message blocks" is shown in '095 col. 7, lines 60-67 "FIG. 2 illustrates a data processing network 40 in which the present invention may be practiced. The data processing network 40 includes a plurality of individual networks, including LANs 42 and 44, each of which includes a plurality of individual workstations 10. Alternatively as those skilled in the art will appreciate, a LAN my comprise a plurality of intelligent workstation coupled to a host processor"

"to one operation unit and assigning said number of random number sequences to another operation unit" is disclosed I '095 col. 17, lines 13-30 "The equations for the subrounds have been present generally in numerical order of the data word affected for that subround, except where the feedback operations required a different order. The order in which the operations are depicted in FIG. 4 does not correspond exactly to the order of the equations: for drawing convenience, FIG. 4 sometimes shows the operations in a different order so that the 3 output lines of the expansion box (shown as arrows leaving the square box) do not cross each other. Because the 3 subrounds which use the expansion box outputs are independent of each other, the order of these subrounds is irrelevant".

As to independent claim 13, this claim is directed to the apparatus of the method of claim 1, and therefore is rejected under the same rationale.

As to independent claim 25, this claim is directed to a medium storing a program of the method of claim 1, and therefore is rejected under the same rationale.

As to independent claim 37, this claim is directed the program product of the method of claim 1, and therefore is rejected under the same rationale.

As to dependent claims 14-20 and 26-32, these claims contain substantially similar subject matter as claims 2-8 and are rejected along the same rationale.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ober et al.	U.S. Patent No. 6,708,73	issued 03/16/2004

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. "**After 26 October 2004, the examiner can be reach at (571) 272-3842".** The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
1 September 2004

NORMAN M. WRIGHT
PRIMARY EXAMINER